Public Interest Energy Research (PIER) Program
FINAL PROJECT REPORT

ADVANCED DISTRIBUTED SENSOR NETWORKS FOR ELECTRIC UTILITIES

Prepared for: California Energy Commission
Prepared by: Science Applications International Corporation

From Science to Solutions

JUNE 2012
CEC-500-2012-069

Prepared by:

Primary Author(s):
J. Roger Bowman
Darrin Wahl

Science Applications International Corporation
10260 Campus Point Dr.
San Diego, CA 92121
858-826-9507
www.saic.com

Contract Number: 500-06-050

Prepared for:

California Energy Commission

David Chambers
Contract Manager

David Chambers
Project Manager

Mike Gravely
Office Manager
Energy Systems Research Office

Laurie ten Hope
Deputy Director
RESEARCH AND DEVELOPMENT DIVISION

Robert Oglesby
Executive Director

DISCLAIMER

This report was prepared as the result of work sponsored by the California Energy Commission. It does not necessarily represent the views of the Energy Commission, its employees or the State of California. The Energy Commission, the State of California, its employees, contractors and subcontractors make no warrant, express or implied, and assume no legal liability for the information in this report; nor does any party represent that the uses of this information will not infringe upon privately owned rights. This report has not been approved or disapproved by the California Energy Commission nor has the California Energy Commission passed upon the accuracy or adequacy of the information in this report.

PREFACE

The California Energy Commission Public Interest Energy Research (PIER) Program supports public interest energy research and development that will help improve the quality of life in California by bringing environmentally safe, affordable, and reliable energy services and products to the marketplace.

The PIER Program conducts public interest research, development, and demonstration (RD&D) projects to benefit California.

The PIER Program strives to conduct the most promising public interest energy research by partnering with RD&D entities, including individuals, businesses, utilities, and public or private research institutions.

PIER funding efforts are focused on the following RD&D program areas:

- Buildings End-Use Energy Efficiency
- Energy Innovations Small Grants
- Energy-Related Environmental Research
- Energy Systems Integration
- Environmentally Preferred Advanced Generation
- Industrial/Agricultural/Water End-Use Energy Efficiency
- Renewable Energy Technologies
- Transportation

Advanced Distributed Sensor Networks for Electric Utilities is the final report for the Advanced Distributed Sensor Networks for Electric Utilities project (agreement number 500-06-050) conducted by Science Applications International Corporation. The information from this project contributes to PIER's Energy Technology Systems Integration Program.

For more information about the PIER Program, please visit the Energy Commission's website at www.energy.ca.gov/research/ or contact the Energy Commission at 916-327-1551.

ABSTRACT

The primary objective of this project was to demonstrate a system to detect intruders and environmental hazards at electric transmission towers and substations using a new generation of distributed sensor networks based on advanced wireless mesh networking technology. A secondary objective was to demonstrate the dual-use capability of wireless mesh sensor systems to monitor the state of health of components of the transmission system. This project designed and fabricated two types of wireless sensor nodes, one with geophones and magnetometers, and another with passive infrared detectors, accelerometers and thermistors. This project developed software algorithms to fuse detection data from multiple sensor nodes to achieve a high probability of detection while minimizing false alarms. This project also developed a graphical interface that displays the alarm status from the data fusion process, sensor node state of health, and temperatures and transformer differential temperature. This project deployed and demonstrated a network of 89 wireless sensors on and around two switchyards, three adjacent transmission towers and a nearby storage yard at an San Diego Gas and Electric (SDG&E) transmission substation. The system successfully detected and localized simulated threats in six scenarios, including intrusion, tampering and wild fire. During a 15-day period, the system made only three potentially false alarms.

Keywords: Public Interest Energy Research (PIER) Program, sensor, wireless mesh network, intrusion detection, electric transmission

Please use the following citation for this report:

Bowman, J. Roger, Darrin Wahl. (Science Applications International Corporation). 2011. ***Advanced Distributed Sensor Networks for Electric Utilities.*** California Energy Commission. Publication number: CEC-500-2012-069.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Introduction

This report describes the Advanced Distributed Sensor Networks for Electric Utilities Project, which was conducted by Science Applications International Corporation between August 2007 and June 2009.

Purpose

The broad purpose of this project was to demonstrate the potential application to the electrical transmission system of a new generation of distributed sensor networks based on very low power advanced wireless mesh networking technology.

Project Objectives

The primary objective of this project was to demonstrate a system to detect intruders and environmental hazards at electric transmission towers and substations using a new generation of distributed sensor networks based on advanced wireless mesh networking technology. A secondary objective was to demonstrate the dual-use capability of wireless mesh sensor systems to monitor the state of health of components of the transmission system.

Project Outcomes

This project designed and fabricated two types of small, battery-powered wireless sensor nodes, one with geophones and magnetometers, and another with passive infrared detectors, accelerometers and thermistors. The geophone/magnetometer sensor nodes are designed to be buried in the ground. They detect ground motion from pedestrians and vehicles, and they detect changes to the magnetic field caused by the passage of vehicles. The passive infrared/accelerometer/thermistor sensor nodes are intended for mounting above ground. They detect the motion of intruders and vibrations on perimeter fences, transmission towers, and transformers resulting from intrusion or tampering, and they sense temperatures and differential temperatures for detection of extreme environmental conditions, including wildfire and transformer state of health.

This project deployed a network of 89 wireless sensors on and around two switchyards, three adjacent transmission towers, and a nearby storage yard at a San Diego Gas & Electric transmission substation. This project demonstrated this system to the Technical Advisory Committee. The system successfully detected and localized simulated threats in six scenarios, including intrusion, tampering, and wild fire. During a 15-day period, the system made only three potentially false alarms.

Conclusions

The system developed by Science Applications International Corporation successfully met the project objectives. This project demonstrated that:

- Wireless mesh networking provides an effective communication framework for operation in power transmission environments, despite the harsh Electromagnetic Interference environment due to high voltages and Radio Frequency obstructions.

- Wireless mesh networking allows very cost-effective installation of a monitoring system.
- Wireless mesh networking allows flexible and cost-effective modification and augmentation of an existing monitoring system.
- Wireless mesh networking provides a cost-effective method for monitoring transmission towers.
- Ultra-low power wireless mesh networking provides low maintenance costs based on multi-year lifetimes using replaceable batteries.
- Fusion of detections from a network of sensors produces effective detection of intrusions with a very low false alarm rate.

Recommendations

In order to facilitate production and successful transition of the technology to electric utility providers of California, the authors recommend a demonstration of a multi-purpose “smart dust” wireless sensor network for the utility industry (including a long linear network, ~10 km, associated with transmission lines) combined with a comprehensive plan for production and transition.

Benefits to California

The results of this project could be applied to increase the reliability of the delivery of electricity to Californians. The electric transmission system of California is vulnerable to damage from deliberate attacks and from environmental hazards, such as wildfires, yet the transmission system is not generally monitored for intrusion, tampering, or environmental hazards. Wireless sensor networks provide a cost-effective approach for broad monitoring to provide rapid notification of potential threats to the transmission system. Traditional wired instruments are difficult and expensive to install to monitor the state of health of high value assets in transmission substations because of the cost of running cables and the need to protect them from the high voltages in the area. In contrast, wireless sensor networks can be installed easily because they form a communication network on their own to route sensor data to a central monitoring location and they are immune to the high voltages in the substation. Transmission towers are currently unmonitored for potential threats because their wide spacing and distribution in remote areas has made it impractical to transmit sensor data to a central monitoring location. Wireless sensor networks allow monitoring a series of adjacent towers with a single wireless network. Real-time monitoring of transmission substations and towers allows utilities to respond rapidly to threats, thereby increasing the reliability of the electric system and reducing the cost of maintaining it.

1.0 Introduction

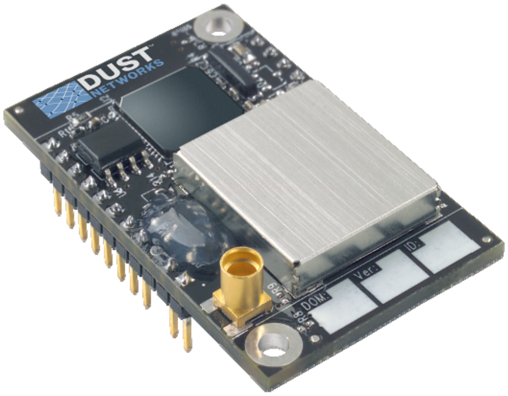
This report describes the Advanced Distributed Sensor Networks for Electric Utilities Project, which was conducted by Science Applications International Corporation (SAIC) between August 2007 and June 2009. The broad purpose of this project was to demonstrate the potential application to the electrical transmission system of a new generation of distributed sensor networks based on advanced low-power wireless mesh networking technology.

The electric utility system is vulnerable to outages due to a range of causes, including natural disasters, accidental damage, vandalism, and terrorism. The main risk from a successful terrorist attack would be widespread power outages lasting an extended period of time. Two primary vulnerabilities are high-voltage transformers and transmission towers (Abel 2005). Recovery from a transformer failure can take weeks to months. Recovery from damage to an individual transmission tower is more rapid, but contemporaneous and widespread attack could lead to significant outages. The Department of Homeland Security (DHS) reported that four separate attacks occurred to transmission towers (bolts were removed) in northern California and Oregon during a four-day period in October 2003 (DHS, 2003). Similar attacks were reported on high voltage transmission lines near Reno, Nevada in December 2004 (HSOC, 2004). Numerous similar attacks have occurred in Colombia (Anonymous, 2004).

For these reasons, the electricity transmission infrastructure is considered by the California Energy Commission (ENERGY COMMISSION) to be one of the highest priority security research topics. Currently, it is extremely challenging to ensure the security of electricity transmission towers as the geographically extensive transmission line systems make large-scale deployment and operation of traditional security measures cost prohibitive. Transmission substations are also considered by the ENERGY COMMISSION to be a high priority area for security upgrade. Currently, some substations have in place perimeter security measures such as optical fiber and closed-circuit television for intrusion detection purposes. However, current practice requires control room personnel to monitor the security screen at all times.

Smart Dust wireless mesh networks, which have emerged from over $100M investment by the Department of Defense over the last decade, offer significant potential for practical and affordable security of the electricity transmission infrastructure (Talbot 2005; Hatler and Chi 2005). Physical intrusion detection is recognized as a key application of Smart Dust by the Science and Technology Directorate of the Department of Homeland Security to protect our Nation's critical infrastructure (DHS, 2005). Figure 2 shows an example of a Smart Dust "mote" from Dust Networks. A mote is a commercial wireless networking device for ultra-low-power, self-configuring, self-healing wireless mesh networks . SAIC is on the leading edge of integrating, developing and exploiting Smart Dust wireless sensor networks that include motes, various sensors, power options, antennas, and data processing and fusion algorithms and software. This project leveraged a 3-year investment and success on several DoD programs to demonstrate a cost-effective solution to securing the electricity transmission infrastructure.

Figure 1. Smart Dust mote from Dust Networks



.

1.1. Objectives

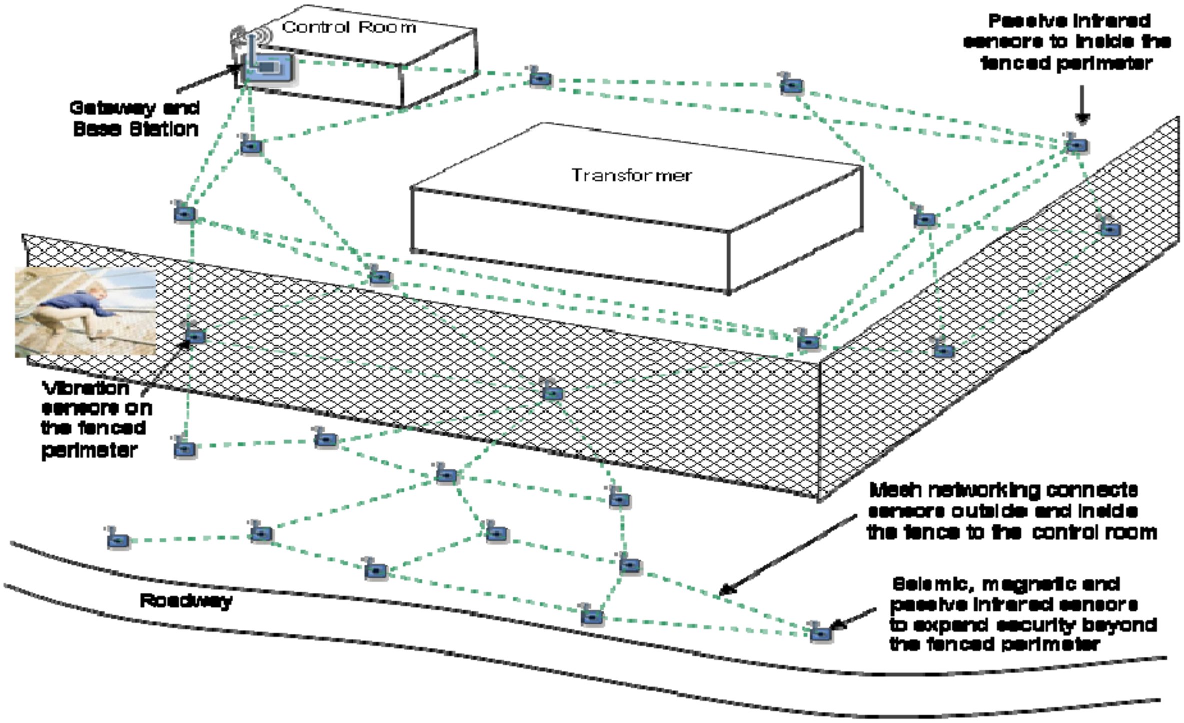
The broad purpose of this project was to demonstrate the potential application to the electrical transmission system of a new generation of distributed sensor networks based on advanced low-power wireless mesh networking technology. More specifically, the primary objective was to demonstrate a system to detect intruders and environmental hazards at electric transmission towers and substations using a new generation of distributed sensor networks based on this technology. A secondary objective was to demonstrate the dual-use capability of the wireless mesh sensor systems to monitor the state of health of components of the transmission system.

1.2. Monitoring Concept

The concept for securing the transmission substation and towers is to provide a sequence of monitoring layers to expand the radius of the current physical security system beyond the fence line in areas of vulnerability and provide early detection and warning of an intrusion or tampering to the control room staff. Because the basic sensors, sensor data processing, network data fusion, and mesh networking requirements are similar for the transmission tower and substation security applications, the same basic intrusion detection system is used for both applications.

Figure 3 shows the concept applied to a transmission substation. Detections from the sensor network (outside the perimeter, on the fence itself, and inside the perimeter) are fused into timely and actionable alarms for control room security staff. Seismic and magnetic sensors are placed outside the fence along expected approach paths to warn the operators of a possible encroachment. Vibration sensors are placed on the fence to warn of climbing or cutting. Passive infrared sensors inside the perimeter detect intruders that have successfully breached the fence. Vibration sensors are also placed on high-value assets to detect shooting at the equipment from outside the substation. The multi-hop wireless mesh networking enables reliable communication within the perimeter of the transmission substation, where point-to-point communication would be unlikely to succeed.

Figure 2. Monitoring system concept for transmission substation security


Control Room
Passive infrared sensors to inside the fenced perimeter
Gateway and Base Station
Transformer
Vibration sensors on the fenced perimeter
Mesh networking connects sensors outside and inside the fence to the control room
Seismic, magnetic and passive infrared sensors to expand security beyond the fenced perimeter
Roadway

The concept is applied similarly to monitoring of transmission towers. Seismic and magnetic sensors are placed around the base of the towers to detect approaching pedestrians and vehicles. Vibration and passive infrared sensors are deployed on the towers to detect tampering such as unbolting the tower from its mounting points or cutting the tower at its mounting or structural support points. Detections made by the sensors are reported via the sensor network to the control room where they are presented to operators as actionable information. Sensors are deployed at several consecutive towers and integrated into one wireless mesh sensor network. A series of towers and substations can be monitored this way with a single gateway (data exfiltration point).

In addition to security monitoring, sensor nodes with temperature sensors are deployed on high-value assets such as transformers to monitor equipment state of health (temperature and differential temperature) and on transmission towers to detect natural disasters such and fire and extreme cold.

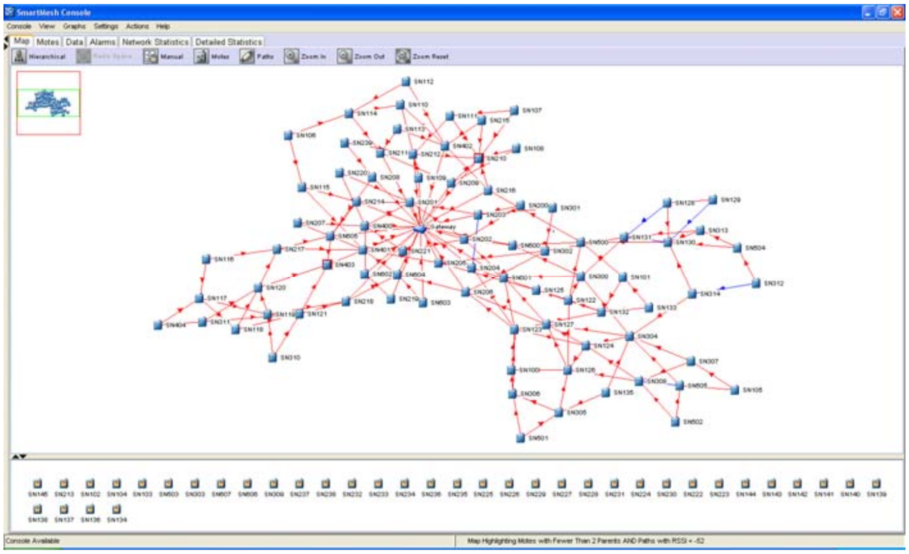
1.3. Wireless Mesh Networks

Wireless mesh network technology has been designed to optimize bandwidth utilization to minimize power usage while providing high reliability of data delivery. This allows deployment of low-cost, easily deployed, long lifetime networks that can relay information about the status and health of power systems to improve timely management of their performance and thereby reduce costs. Smart Dust mesh networks combine sophisticated mesh networking software and low-power wireless nodes ("motes") to provide very high reliability, manageability and ease of installation. These self-healing networks provide high-reliability data delivery and network extent unavailable with peer-to-peer networks. A unique aspect of Dust Networks Inc.'s technology deployed in this project is its very precise time synchronization that supports full mesh networking in a battery-powered network, unlike other mesh networks that require continuously powered routing nodes (known as star-mesh). This precise time synchronization allows deep duty cycling for all nodes, even for routers, which allows lifetimes of years on disposable batteries. This is particularly important for a linear network deployment, such as would be used along power lines; in this case, most of the nodes will act as data routers as well as support sensors (Figure 4). Wireless mesh network features and benefits are summarized in Table 1.

Table 1. Characteristics of Wireless Mesh Networks

Key Feature	Benefit
Wireless	Unaffected by induced currents in the electromagnetic environment
Low cost	Affordable large networks; data fusion improves detection performance and mitigates false alarms
Ultra low power	Long lifetime (years with lightweight batteries); very low maintenance
Self-configuring	Easy and inexpensive to deploy
Self-healing and redundant routing	High reliability
Multi-hop mesh networking	Scalable – long reach over large terrains
Interface for analog and digital sensors	Flexible – supports multiple sensor types in one network
Open standards	Easy integration with legacy systems (e.g., SCADA).

In addition to security of the transmission infrastructure, Smart Dust mesh networks have significant potential for dual use in the electric utility industry (e.g., transformer health monitoring, line temperature monitoring, and fault current indication) due to their flexibility to add new sensor nodes to an existing network. Exploiting the wireless mesh networking infrastructure of the security monitoring system for multiple purposes will improve its overall cost-effectiveness.



Console Available

Map Highlighting Motes with Fewer Than 2 Parents AND Paths with RSSI < -52

Figure 3. Connection topology of the wireless mesh network at the demonstration site

1.4. Technical Advisory Committee

Execution of this project was overseen by a Technical Advisory Committee consisting of representatives of stakeholder organizations:

- California Energy Commission
- San Diego Gas & Electric (SDG&E), a key partner
- Pacific Gas and Electric
- California Independent System Operators
- California Emergency Management Agency
- Science Applications International Corporation

The Technical Advisory Committee met at SAIC's office in San Diego for a kickoff meeting, a System Requirements Review, and a System Design Review. The committee also attended a Test Readiness Review and witnessed the demonstration of the Advanced Distributed Sensor Network System when deployed on the SDG&E transmission system.

2.0 Project Approach

The demonstration system for this project was based on a prototype wireless sensor system that was developed for the U.S. Marine Corps. This project followed a systems engineering approach to adapt and extend the system to monitor electric transmission systems. This project first analyzed the requirements of threat monitoring for the electric transmission system and conducted a detailed survey of the demonstration site. This project then designed and developed the demonstration system to meet the system requirements. The requirements, design, and development are described in this section.

2.1. Requirements and Site Survey

The context of the environment in which the Advanced Distributed Sensor Networks for Electric Utilities System (the system) operates is depicted in Figure 5. The system is shown as the blue box in the center; external entities as the grey boxes; and users as the yellow box. The system senses intruders, tampering, and environmental hazards. Additionally, the project evaluated the dual-use potential for sensing characteristics of the electric transmission system. The system must operate in the physical environment, including weather, electrical field, vegetation, and the built environment. Users interact with the system through a graphical user interface.

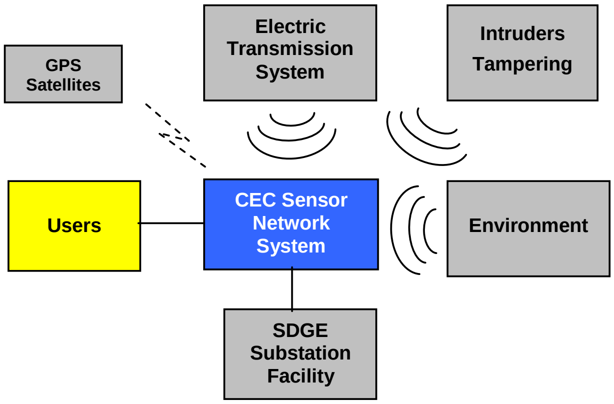


Figure 4. System context

2.1.1. User Requirements

The primary objective of this system is to alert users to intrusion, tampering and environmental hazards. High-level user requirements are presented in Table 2. Note that this document and project define the terms “detection” to be the automated recognition of a changed state at an individual sensor and “alarm” to be the automated recognition of a possible threat inferred from a pattern of detections at one or more sensor(s) that match the physical and spatial characteristics of a possible threat.

Table 2. User Requirements

Number and Name	Requirement
UR 1 Intrusion alarm	Detect human intruders (pedestrian or vehicles) at transmission towers and substations.
UR 2 Tamper alarm	Detect human activities that may damage transmission towers.
UR 3 Environmental hazard alarm	Detect environmental conditions that may damage transmission towers or degrade transmission performance.
UR 4 Location of alarms	Locate detected intruders, tampering activities, and environmental hazards.
UR 5 Characterization of alarms	Characterize detected intruders, tampering activities, and environmental hazards.
UR 6 Alarm reporting	Report occurrence, location and characterization of intrusion, tampering and hazards to user.
UR 7 Dual-use potential	Demonstrate potential of security system to monitor the condition or state of health of components of the electric power transmission system.
UR 8 Low-cost installation and O&M	Demonstrate potential for system to have low installation, operations and maintenance costs.

Detailed systems requirements are defined in Demonstration System Requirements and Site Survey Report for the Advanced Distributed Sensor Networks for Electric Utilities Project (Bowman et al., 2008).

2.1.2. Concept of Operations

The concepts of operations for demonstrating the prototype system during this project and for a future, operational system are defined here.

Demonstration of Prototype System

The prototype system operated in the vicinity of SDG&E equipment, but was independent of their security and equipment monitoring systems. The system spanned the transmission substation and an adjacent, contiguous set of transmission towers. The system's base station (operator console) was deployed in an SDG&E building (control room) within one of the substation switchyards.

The prototype system operated autonomously, making detections at individual sensors, processing the detection data to declare event alarms, and logging detections, alarms and system state of health in a database of the base station. Users reviewed the alarms on-site at the substation.

The demonstration had two components: active tests and passive tests. The active tests demonstrated the system behavior in response to specific stimuli. The passive tests characterized the false alarm behavior. The system performance was observed at the base station immediately following each element of the active tests. For the passive tests, the system operated unattended for two weeks, logging to the base station database. The results of the passive tests were then derived from the database of the base station.

Operational Systems

In contrast to the prototype system, future operational systems for intrusion detection and monitoring of state of health of the transmission system will likely be integrated with the electric utilities' existing security and control systems (e.g., SCADA). Data and results of data analysis will then be transmitted from the locations of the deployed sensors to a central facility where they can be available for integration into the utility's monitoring and response procedures.

2.1.3. Site Survey

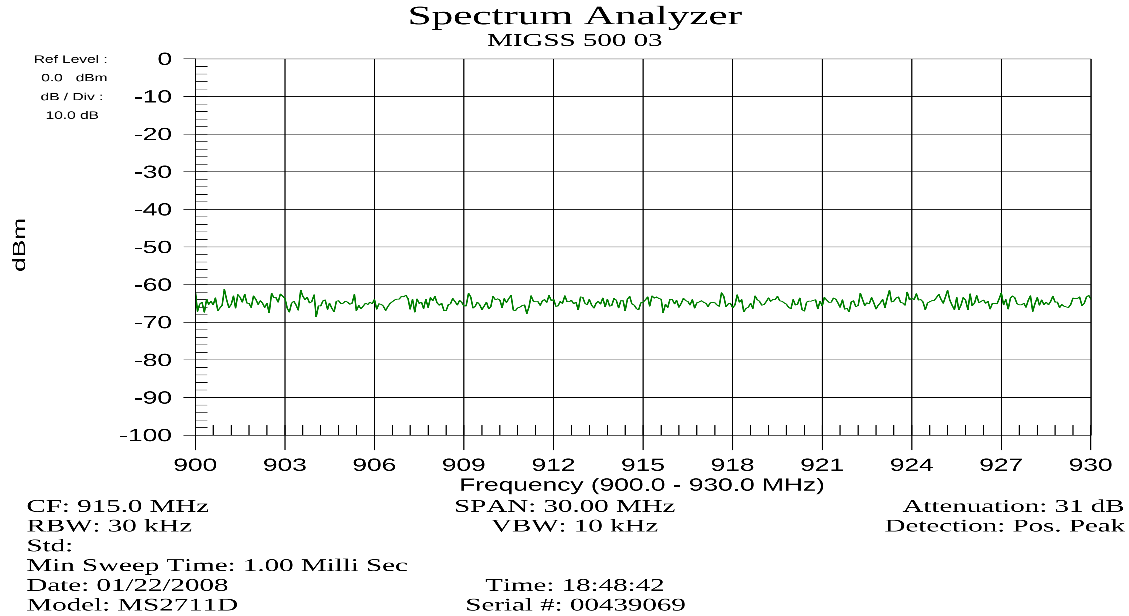
SAIC conducted a survey of the demonstration site on January 22, 2008 (Bowman et al., 2008). The survey applied the Department of Energy's Energy Infrastructure Vulnerability Survey Checklists (Office of Energy Assurance, 2002).

The perimeter fences at two switchyards at the demonstration site are well installed and appear to be in good condition. The perimeter fence at the storage yard, where some copper theft has occurred previously, shows signs of wear and tear. Several spots on the fence fabric have been patched after breaches. That same fence uses wooden slats interwoven with the fabric to provide a visual barrier to the electrical equipment stored in the yard. The wooden slats can also provide coverage for intruders breaking into the facility. The two switchyards each have a concrete lined drainage ditch, an added physical barrier that is constructed for environmental protection but adds a degree of protection to the perimeter barrier. These ditches could add a significant delay to any vehicle-borne attack on the perimeter fence because of its depth and breadth.

A variety of monitoring equipment is deployed in the switchyards and storage yard, including closed-circuit television (CCTV) cameras, infrared (IR) illuminators, and passive infrared (PIR) detectors. Each of the three yards has multiple layers of intrusion detection systems: fiber optic cable woven into the fence around the entire perimeter, passive infrared detection at the main gate, and CCTV cameras with infrared illuminators at specific locations. The storage yard also combines passive infrared and microwave detection at the main gate and a secondary vehicle gate. When an alarm is activated, a warning signal comes on inside the yard at the control room, and an alarm is sent to a central security station. Roving security guards are then alerted to check out the alarm at the substation.

Measurements were made within the switchyards and the storage yard for the purpose of identifying electromagnetic interference (EMI) with the transmission of radio-frequency signals in the 900-928 MHz range used by the wireless mesh network for the demonstration system.

Using a spectrum analyzer equipped with a 900 MHz range antenna, instantaneous measurements were made at various locations throughout the switchyards and the storage yard, including directly under high-voltage transmission lines, within 1 m of transformers and capacitors, and directly beneath the microwave communication antenna tower in the small switchyard. In all locations, the background power level in the frequency band of interest was approximately -65 dBm, which is the same as that observed in a typical building parking lot. A typical measurement in the 900-928 MHz range, in this case taken directly beneath transmission lines (height approximately 10 m), is presented in Figure 6.



CF: 915.0 MHz
SPAN: 30.00 MHz
Attenuation: 31 dB
RBW: 30 kHz
VBW: 10 kHz
Detection: Pos. Peak
Std:
Min Sweep Time: 1.00 Milli Sec
Date: 01/22/2008
Time: 18:48:42
Model: MS2711D
Serial #: 00439069

Figure 5. Typical spectrum measured within the small switchyard

In addition to spectral measurements, small wireless mesh networks were deployed in a multi-hop configuration to test whether network nodes could communicate in the 900-928 MHz range within the switchyards. Measurements of the received signal strength and path stability were recorded at the maximum separation distances, and values were within acceptable levels for successful operation of a wireless mesh network.

In addition to EMI, poor line of sight and multi-path effects can also interfere with radio communications. Line of sight within a switchyard is typically unobstructed over short distances (10-20 m), but is somewhat obstructed by the steel structures and steel and concrete buildings. Wireless mesh network testing indicated that line of sight and multi-path effects were not a problem.

2.1.4. Adjacent Transmission Towers

The transmission towers adjacent to the substation are galvanized steel lattice structures built to support overhead AC transmission lines that carry three-phase current. The towers approach the substation from the east as seen in the lower right of Figure 7.

Vehicles and pedestrians can access the area containing the transmission towers by the same methods described for the substation: via the front access gate, via several dirt roads from the east and south, or via the open space surrounding the region. Unauthorized vehicle or pedestrian access is possible but hindered by the sloped and hilly terrain. Towers 23 and 24 have dirt roads leading to their bases. Tower 22 has a dirt walking path leading up to its base.

Each tower is about 35 m tall with a 10 m square base. A tower’s four legs are mounted in concrete and have a horizontal stabilizing structure about 10 m up and climbing pegs on one of the four legs.

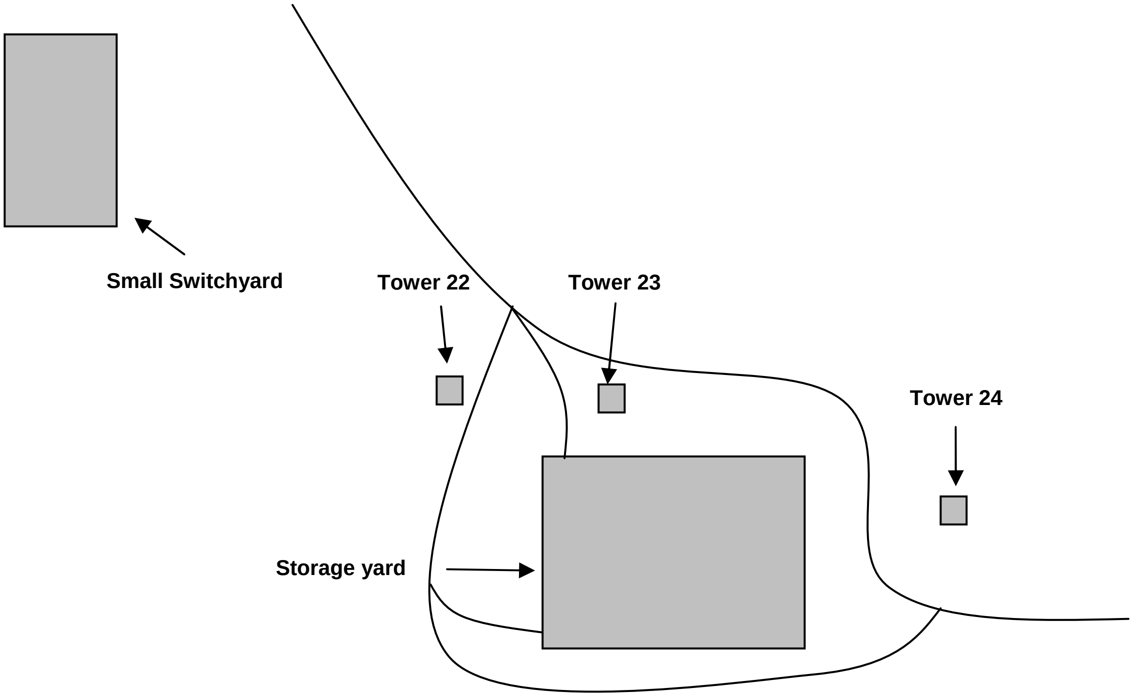


Figure 6. Relative locations of transmission towers

There are no security systems or perimeter barriers for any of the transmission towers. Each tower’s four legs are anchored in concrete, with 15-20 0.5 in bolts securing each panel near the base (Figure 8). Most of the bolts have collars that would impair the use of a socket wrench to remove the nut. There is no evidence of spot welding of nuts to bolts to prevent removal of the nuts.

The towers are constructed of galvanized steel angle iron approximately 0.25 in thick, 3 in wide. Wireless sensor nodes could be attached to lattice elements using strong magnets. For permanent installation, sensor nodes could be attached by bolting or strapping to the lattice elements.

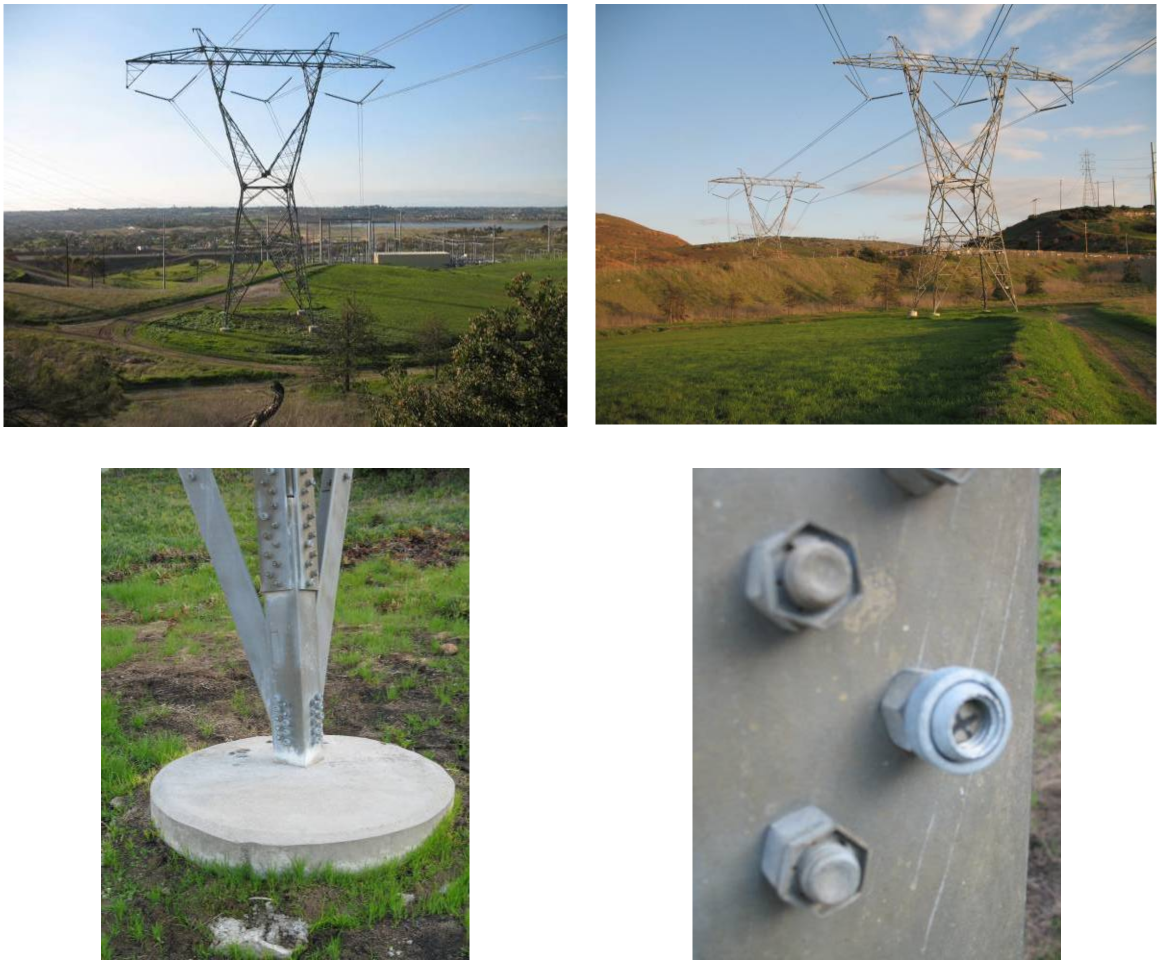


Figure 7. Photographs of transmission towers adjacent to small switchyard. Upper Left: Tower 22 looking west toward the small switchyard. Upper Right: Tower 22 looking east toward Tower 23 and the storage yard. Lower Left: Tower leg anchored in concrete. Lower Right: Bolts with collars to prevent removal.

EMI measurements were made near the transmission towers and under transmission lines using the same methods described for the switchyards. In all locations, the background power level in the frequency band of interest was approximately -65 dBm, which is the same as that observed in a typical building parking lot and in the switchyards.

Line-of-sight (LOS) and multi-path effects are more problematic over the longer distances between towers, between switchyards, and between towers and switchyards. Tower 23 sits about 10 m below the storage yard access road, and, thus, its base has an obstructed LOS to the lower part of Tower 22. However, the LOS from Tower 22 to the small switchyard is unobstructed. The LOS from the base of Tower 24 to the base of Tower 23 is somewhat obstructed by vegetation and the height differential.

2.2. System Design and Development

This section presents a high-level view of the design of the system. First, the system architecture is presented. Next, the design is presented for each of the major subsystems: sensor nodes, gateways, and the base station. Finally, the development and fabrication of the system is discussed.

2.2.1. System Architecture

The system architecture consists of sensor nodes, a gateway, a base station, and support equipment as depicted in Figure 9. The sensor nodes sense the environment, detect signals, and communicate with other sensor nodes and/or gateways via short-haul radio. The gateways receive information from the network of sensor nodes and communicate with a base station via Ethernet. The base station performs data processing, interpretation, visualization, and network command and control, as well as providing the primary interface to external systems.

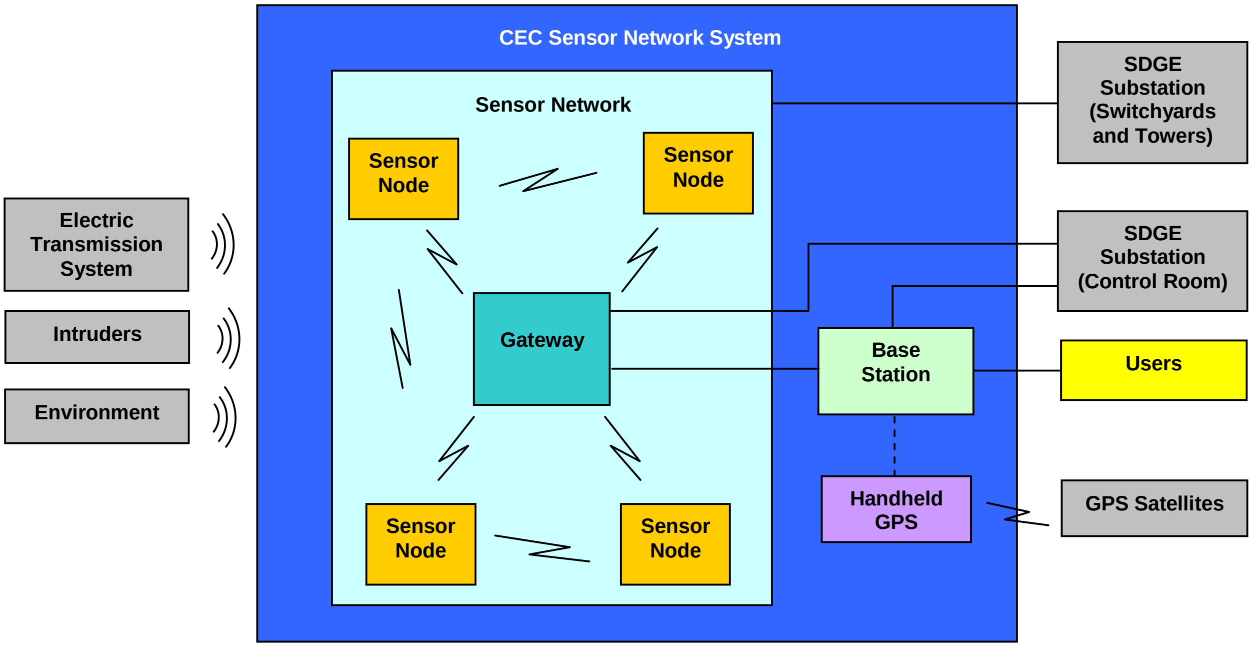


Figure 8. System architecture of the Advanced Distributed Sensor System. The system is shown within the dark blue box. External entities are shown as gray boxes and users as a yellow box.

2.2.2. Sensor Nodes

As depicted in Figure 10, each sensor node consists of a mote integrated with a sensor, a sensor data processor, batteries, and a radio antenna in a package designed to meet deployment and environmental requirements. The sensor processor performs analog-to-digital conversion and signal processing on the sensor input and then provides sensor information to the mote. For most sensors, the sensor information consists of detection parameters, such as time of detection and amplitude. For the thermistor (temperature sensor), the information consists of a temperature value. The mote formats the sensor information and transmits it to the network via the antenna. The mote also accepts command and control information from the gateway and forwards relevant information to the sensor processor. The motes were manufactured by Dust

Networks, and were version 1.6 (also called SmartMesh XR). The batteries supply power to all sensor-node components.

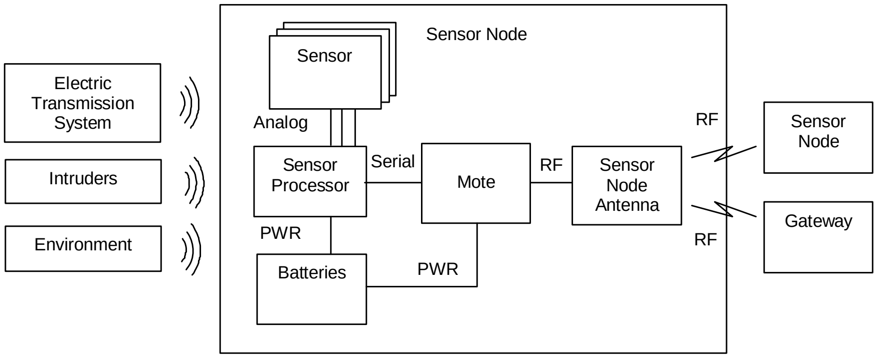


Figure 9. Architecture of all sensor nodes.

This project selected sensors for the sensor nodes that are appropriate to detect target signals, as shown in Table 3. Two types of sensor nodes were designed and fabricated. One type incorporates a geophone and a magnetometer and is intended to be deployed buried in the ground (Figure 11). The second type includes one or two passive infrared (PIR) detectors, an accelerometer, and an optional thermistor (Figure 12). The second type is intended to be deployed above the ground. The geophone, magnetometer and accelerometer are installed inside the sensor node enclosure. In contrast, the PIR and thermistor are mounted outside the enclosure to enable proper sensing.

Table 3. Function of sensors in the system

Sensor type	Purpose
Geophone	Detect vibrations of vehicles, human footsteps.
Magnetometer	Detect presence of vehicles, humans carrying metal objects.
Passive Infrared (PIR)	Detects changes in infrared radiation when there is movement by a person (or object) that is different in temperature from the surroundings.
Accelerometer	Detects static acceleration of gravity in tilt-sensing applications, as well as dynamic acceleration resulting from motion, shock, or vibration.
Thermistor	Detect changes in temperature of air or devices such as transformers.

We selected an enclosure for the sensor nodes that was commercially available and met environmental and size requirements. The Fibox PC 081206 met the IP67 standard for water protection (submersion in up to 1 m of water) and would accommodate the sensor, mote, electronics and two D-cell batteries. Two D-cell batteries provide a lifetime of 3.3 years for the

PIR/accelerometer/thermistor sensor nodes and 1 year for the geophone/magnetometer sensor nodes.

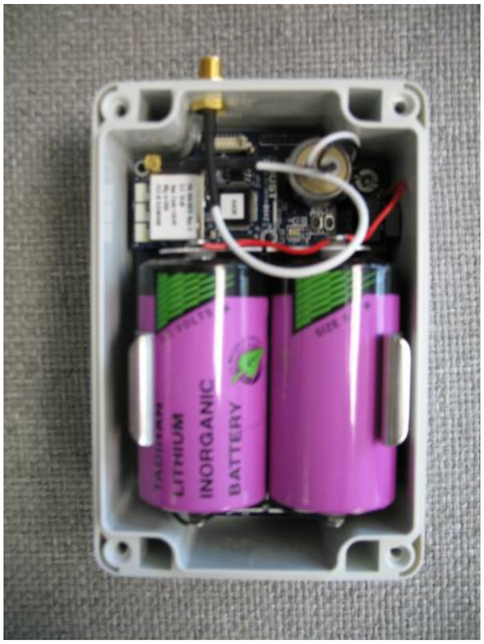


Figure 10. Interior assembly of a geophone/magnetometer sensor node. The geophone is the small disk in the upper right, above the purple lithium batteries.

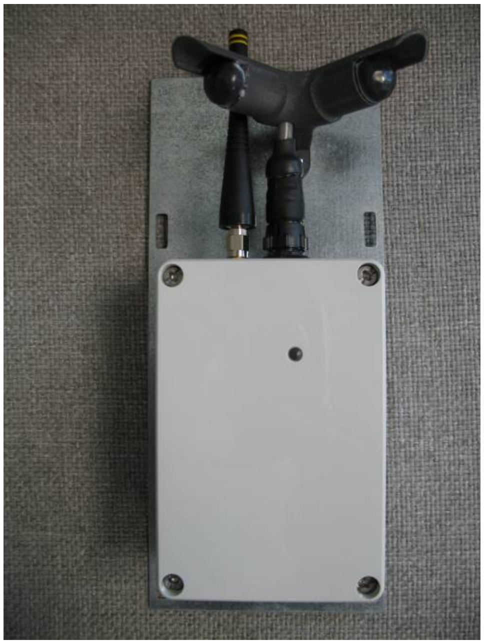


Figure 11. Dual PIR sensors on a sensor node.

This project also considered power harvesting options to assess the feasibility of using alternative power sources for sensor nodes either as a primary power source or as a supplement to conventional batteries in order to extend battery life. Solar power as a primary power source seems feasible, with the exception where covertness is necessary for buried sensors. Rechargeable lithium polymer cells are the best match for requirements based on energy density (Figure 13). Lithium batteries have a specific charging profile that must be used, which requires a charge controller to be added to the sensor node. Flexible solar panels are a good match for outdoor deployment and low power requirements. This project found that a solar panel that would meet requirements would measure 3.7x3.0x.01 inches.

a) Lithium ion rechargeable coin cells **b) Off the shelf lithium polymer cells** **c) Custom thin lithium polymer cell**

Figure 12. Several rechargeable battery options from PowerStream.

2.2.3. Gateway

A system gateway consists of a Dust Networks manager and antenna as depicted in Figure 14. The manager manages the network of sensor nodes. It receives data and status packets from the sensor nodes and forwards them to the base station. The manager receives command and control information from the base station.

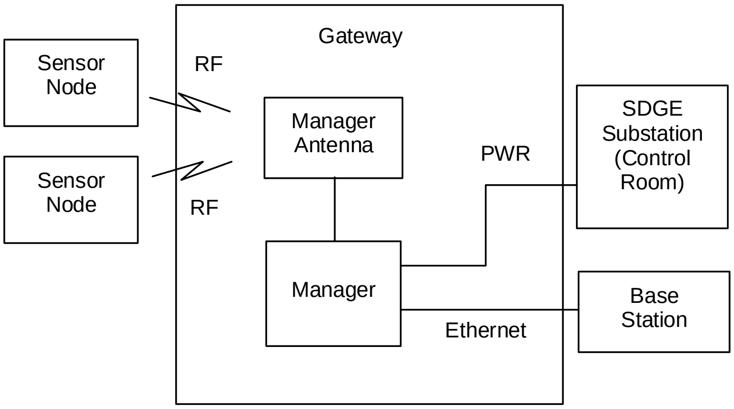


Figure 13. Architecture of the gateway.

2.2.4. Base Station

The architecture of the base station is depicted in Figure 15. The base station is a computer that runs software for data processing, interpretation, visualization, storage, and network command and control, and provides the users a graphical user interface (GUI) for system monitoring. Local commercial power is supplied by the SDG&E substation.

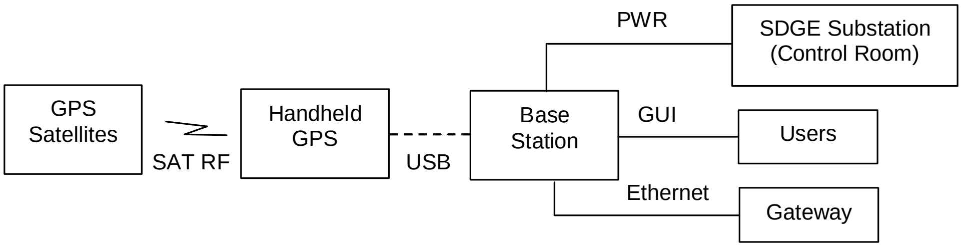


Figure 14. Architecture of base station.

The computer is a standard PC laptop running Windows XP. As depicted in Figure 16, the computer automatically runs data acquisition software to retrieve data from sensor networks. The computer also automatically performs data processing and fusion to detect, locate, and characterize intruders, and to mitigate false alarms. The computer provides command and control software for network initialization, sensor and network configuration, and network state-of-health monitoring. The GUI displays the alarm status of each of the sensor networks and the operational status of system components.

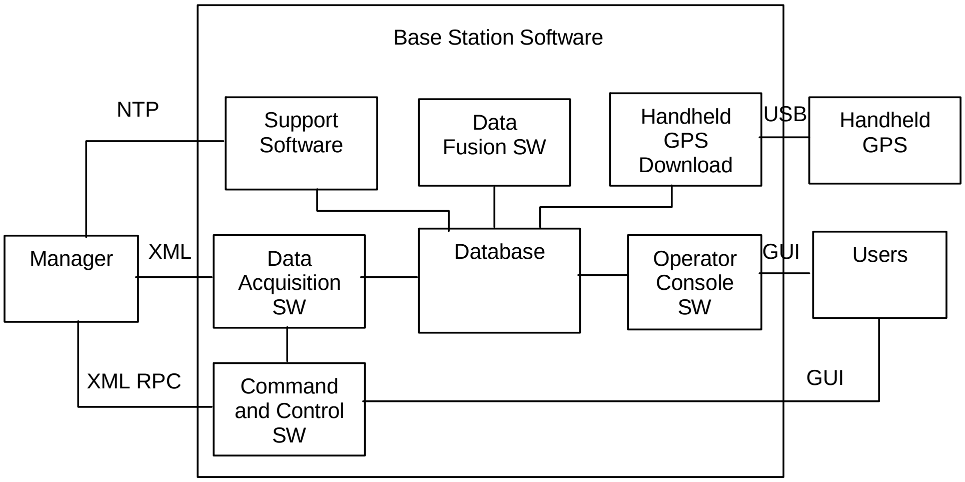


Figure 15. Architecture of base station application software.

Data fusion is the process of taking detections from sensor nodes to form inferences about their cause and decide whether an alarm should be issued. Our solution for this system follows a multi-step approach that first groups detections into “incidents”, which are short duration disturbances such as someone climbing a fence, and then combining sequences of incidents into “events”. Then rules are used to determine whether an alarm should be issued based on the “event”. The use of data from multiple sensor nodes allows the system to achieve a high probability of detection while minimizing false alarms because no single sensor node causes the system to alarm.

2.2.5. Integration

Components of the system were integrated into the system incrementally as they became available. First, the research team installed commercial and shareware components, such as MATLAB and the network time server, on the base station computer. Next, the research team installed application software, including the data acquisition and data fusion applications. Then, the research team attached a single network manager and a set of 10 sensor nodes. This minimal system allowed us to begin rudimentary testing and to make configuration changes necessary for effective end-to-end operation. The research team added additional sensor nodes as assembly of the sensor nodes was completed and updated application software as development was completed.

3.0 Project Results

This section describes the results of integration testing of the system, the field demonstration, and of an analysis of the performance and cost of the prototype system.

3.1. Integration Testing At Demonstration Site

The purpose of integration testing was to verify basic operation of the prototype system in a realistic environment, to adjust system parameters for the local noise environment, and to refine system components as necessary based on the results of testing.

3.1.1. Integration Testing and Demonstration Environment

The demonstration site includes a large switchyard, a small switchyard, a storage yard, and transmission towers. The system operated in the vicinity of SDG&E transmission equipment at the demonstration site, but was independent of SDG&E's currently-deployed monitoring and security systems. The demonstration site is described in detail in the Requirements and Site Survey Report (Bowman et al., 2008). This project conducted integration testing at the demonstration site because it provided the same challenges of EMI, radio range, and potential radio signal blockage that would be encountered during the demonstration.

3.1.2. System Deployment

SDG&E, our key partner on this project, provided access to the demonstration site for system deployment, integration testing and the demonstration. An SDG&E engineer coordinated logistics for the project, which required a "standby" linesman to open the yards and monitor our safety, as well as radio frequency approvals and mounting of sensor nodes at elevation in transmission towers.

On April 6, 2009 this project deployed the system at the demonstration site (Figure 17 to Figure 20). The system consisted of 89 sensor nodes, one gateway and one base station computer. SAIC staff mounted sensor nodes with accelerometers, PIRs, and thermistors on the poles of perimeter fences, mounted sensor nodes with accelerometers and thermistors on transformers, and buried sensor nodes with geophones and magnetometers on approaches to the small switchyard, the storage yard and the transmission towers. A linesman from SDG&E climbed the three transmission towers to mount sensor nodes about 10 m above the ground. SAIC personnel installed the gateway and base station computer in a battery room within the small switchyard and the gateway antenna on the roof of that building.

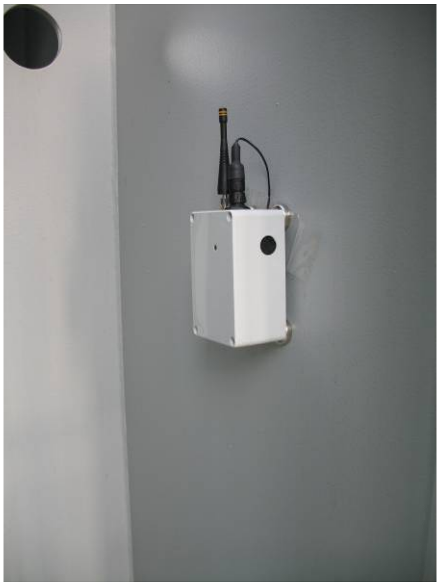


Figure 16. Sensor node with accelerometer and thermistor mounted on transformer.

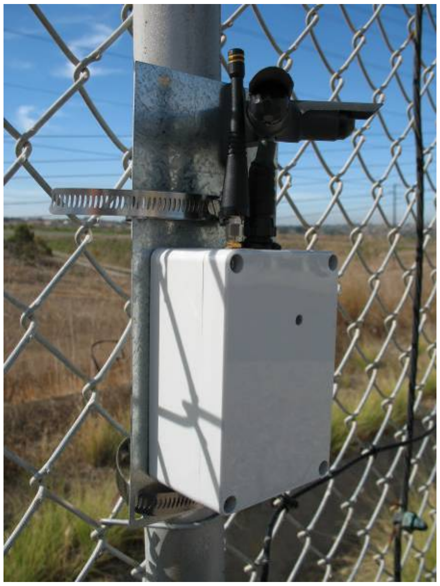


Figure 17. Sensor node with accelerometer and PIR mounted on fence post.

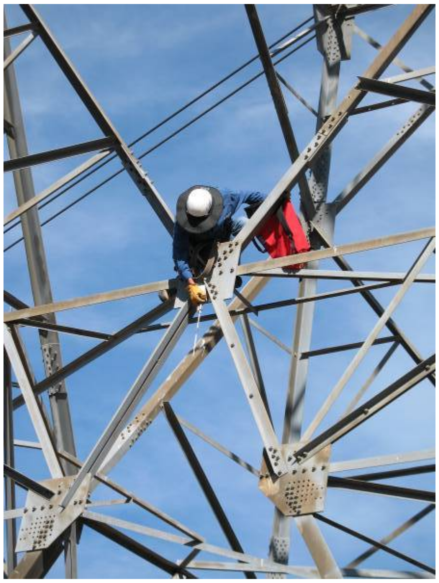


Figure 18. Sensor node (white box with antenna pointing down) with accelerometer and PIR mounted on transmission tower by SDG&E.

Figure 19. Base station computer in work room at small transmission switchyard.

As shown in Figure 20, the system spanned the small switchyard, a stairway between the small and large switchyards, a portion of the large switchyard, the storage yard, an adjacent, contiguous set of three transmission towers, and a three-road fork leading to the towers and storage yard. The distribution of sensors is summarized in Table 4. It is important to note that this system comprised a single wireless mesh network; no communications other than the wireless mesh was required to transmit detection data from the sensor nodes to the gateway and base station.

Table 4. Distribution of Sensor Nodes at the Demonstration Site

Substation Feature	Number
Fence around small switchyard	26
Transformers in small switchyard	6
Road leading to small switchyard	10
Fence around large switchyard	3
Stairs between switchyards	6
Storage yard	4
Main road leading to storage yard	6
Back road leading to storage yard	4
Tower 22	4
Road leading to tower 22	4
Tower 23	4
Road leading to tower 23	4
Tower 24	4
Road leading to tower 24	4

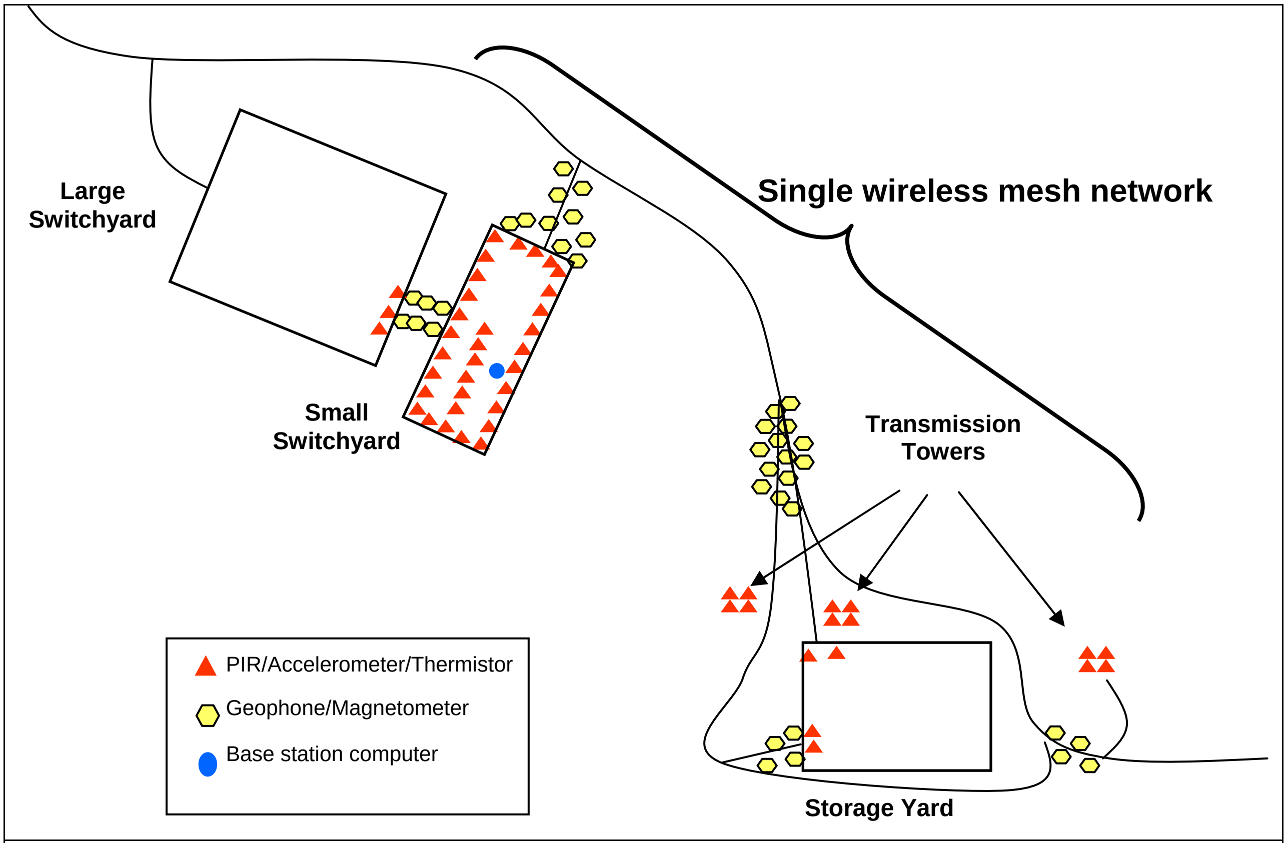
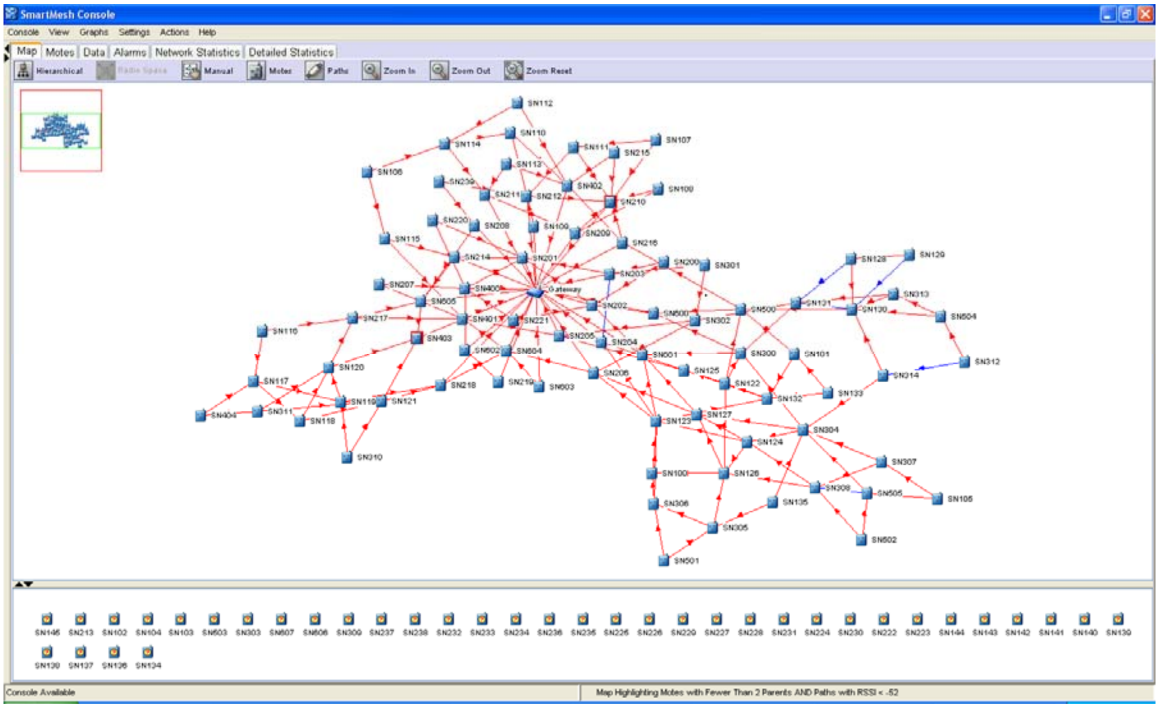


Figure 20. System layout at demonstration site.

3.1.3. Integration Test Results

This project operated the system continuously from April 6 to May 12, the morning of the demo. A key result of this testing was that the wireless network "formed by itself", that is, made connections among sensor nodes, despite the long range (300 m) between the transmission towers and the small switchyard (Figure 21). The line of sight from the gateway antenna (blue circle in Figure 20) to the closest tower was completely blocked by a 10-m high metal building, but the network formed by connecting sensor nodes on the towers to sensor nodes on the perimeter fence. Furthermore, all sensor nodes within the switchyard, including those on the transformers, joined the network, despite obstructed paths.



Console Available

Map Highlighting Motes with Fewer Than 2 Parents AND Paths with RSSI < -52

Figure 21. Connection topology of the wireless mesh network at the demonstration site. Positions of sensor nodes are logical, not physical.

The research team conducted a variety of tests of the detection performance of the system (Figure 22). The initial detection parameters for the buried geophone/magnetometer sensor nodes were inadequate for the two target types, which were pedestrians and vehicles, so the research team reset these parameters remotely over-the-air from the base station. The initial data fusion software was incorrectly computing target azimuths and was not tuned correctly for one type of intrusion alarm, so these errors were corrected. Based on our integration test results, the research team refined the base station software during the period April 6 to 27.

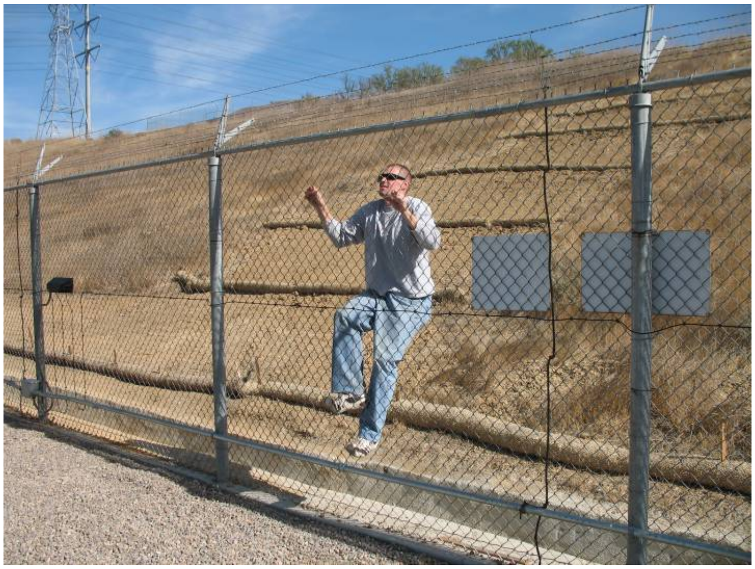


Figure 22. SAIC personnel simulating an intrusion during integration testing.

The research team conducted a dry run of the demonstration tests on April 15. The data collected during the dry run allowed us to make final system refinements. After April 27, the system ran unattended until the demonstration on May 12.

3.2. Demonstration

Between May 12 and 28, 2009 the research team conducted a field demonstration of the prototype system with active testing occurring on May 12 followed by 15 days of passive testing. The system successfully detected simulated intrusions of two switchyards, a storage yard, and transmission towers by vehicles and pedestrians. The system detected simulated tampering with a transmission tower and simulated shooting of a transformer. In addition, the system detected simulated temperature anomalies representative of nearby wildfire, and reported on absolute and differential temperatures of three large transformers. Analysis indicated three possible false alarms during the 15-day period of operation. However, all three of these alarms occurred during business hours on weekdays, but entry into the storage yard is not logged, so it is possible they were false alarms.

The purpose of the field demonstration was to evaluate how the system's wireless mesh networking technology can be employed to satisfy stakeholder needs. The objectives of the specific test cases that were part of the demonstration were to:

- Evaluate how well the system meets system requirements
- Demonstrate the dual-use potential of the wireless mesh networking technology

3.2.1. Demonstration Strategy

The demonstration evaluation of the system was conducted in a realistic setting using potential threat scenarios and for an extended period of time to assess false alarm behavior. In order to accomplish this, the demonstration had two components:

- **Active Test**: This test demonstrated system behavior in response to specific stimuli using scripted events that simulated threat scenarios. Project stakeholders observe system performance at the base station immediately following each element of the active test.
- **Passive Test**: This test was used to characterize the system's false alarm behavior. The system operated unattended for a 15-day period and logged all data to the base station database. The results of the passive tests were then derived from the database.

On May 12, immediately prior to the demonstration, a Test Readiness Review (TRR) was held with the TAC to review test preparations, including results of integration testing, and to determine whether formal testing should proceed (Figure 23). The TAC decided that the test preparations were sufficiently complete to proceed.

Figure 23. The Technical Advisory Committee (TAC) and supporting and SAIC staff during the Test Readiness Review at the demonstration site.

3.2.2. Active Tests

The purpose of the active test was to demonstrate the system's behavior to the TAC. The system was exercised using scripted events that simulated real-world threat scenarios while the TAC witnessed the system's performance at the base station as the events took place (Figure 24 to Figure 26.)

Figure 24. TAC members observe alarms on the system's base station.

Figure 25. TAC member inspecting the temperature histories of transformers in the small switchyard.

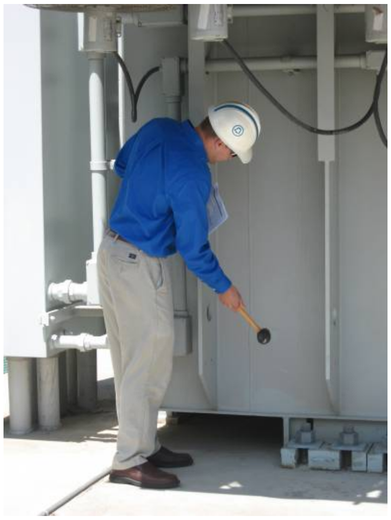


Figure 26. SAIC personnel using a rubber mallet to simulate a bullet hitting a transformer in the small switchyard.

The general order of testing was:

- Simulate intrusion and tampering events at the small switchyard
- Demonstrate dual-use potential at the small switchyard
- Simulate intrusion and tampering events at a transmission tower
- Simulate an environmental hazard at a transmission tower
- Demonstrate mesh networking technology and system capabilities at the storage yard

The system successfully detected all simulated intrusion, tampering and environmental threats. The network communicated the detections to the base station in the control room and the data fusion created alarms based on the detections within 30 to 60 seconds of a scripted event occurring. This data latency on the order of minutes is very low compared to SDG&E's stated response time by authorities of 45 minutes for the demonstration site.

The TAC witnessed all these test scenarios via the system GUI on the base station. The GUI displayed both a high-level view of the entire substation showing the various zones which were instrumented for the demonstration, as well as a close-up view of individual sensor nodes in and around those zones. In a non-alarm state, the sensor nodes were shown as green symbols. In an alarm state, individual sensors that detected movement were indicated by red symbols, and a large red triangle indicated an alarm was formed based on these detections at a particular time and location indicated on the display.

The wireless mesh networking technology provided reliable data transmission across the full 900-m span of the deployed network. In addition, the system was shown to provide the dual-use capability of measuring state of health (differential temperature) of high-value assets in the switchyard (Figure 27).

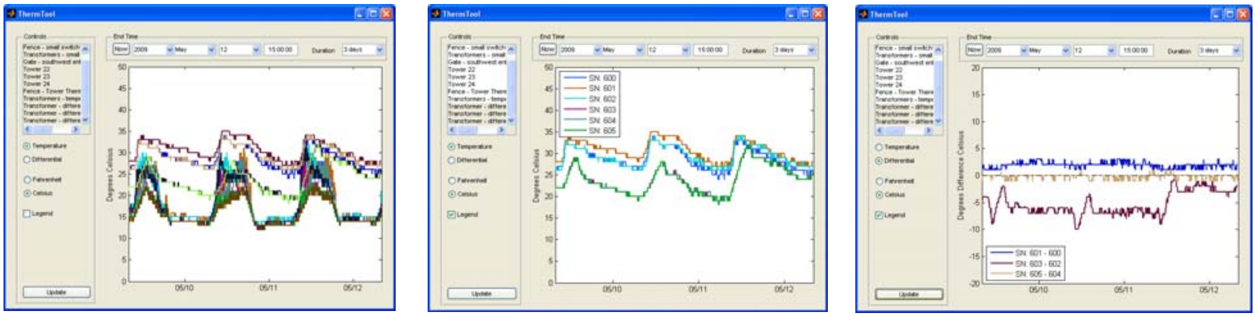


Figure 27. The ThermTool displaying temperature and differential temperature. The image on the left shows the absolute temperature in degrees Celsius as measured by the thermistor sensor nodes (fences, towers, transformers) during a three-day period. The changes in temperature are primarily diurnal variations. The middle image shows the absolute temperature on just the six transformers. The image on the right shows the differential temperature between three pairs of transformers. The red curve on the bottom indicates a larger differential temperature between this pair of transformers than the other pairs.

3.2.3. Passive Test

The system operated unattended for a 15-day period between May 12 and 27 and logged all detection and alarm data to the base station database. The system's false-alarm rate (FAR) was then derived from the database alarm data and security logs of known intrusions (i.e. nuisance alarms).

Our analysis of the system data and security alarms show that the system formed three intrusion alarms at the entrance to the storage yard during "quiet times" during the fifteen day test and none in the other yards or under the three instrumented towers. All three of these alarms occurred during business hours on weekdays, but entry to the storage yard is not logged, so it is also possible they were false alarms.

SDG&E provided three types of activity reports for the complex. These were automated gate entrance logs for the main gate, automated gate exit logs also for the main gate, and self-reported (called in) logs. Not all entrance log entries corresponded to an exit log entry, and many entrance and exit log entries did not correspond to a self-reported log entry. Therefore, the research team infers non-quiet times as the combination of (1) the self-reported activity, (2) entrance log entry time plus two hours, and (3) exit log entry time minus two hours. Not surprisingly, there were a variety of "nuisance alarms" during the "non-quiet" times, that is, when it is highly likely that authorized personnel were in and around the switchyards and storage yard. Notably, there were no nuisance alarms throughout the three-day Memorial Day weekend, which was entirely a "quiet time". The system operated at a very low false alarm rate (less than one/week).

3.3. Performance and Cost Analysis

As part of the project, Sidus Solutions, a security and surveillance solutions provider, assessed the system's performance and cost effectiveness relative to conventional intrusion detection systems. Their assessment is documented in the Performance and Cost Report for the Advanced Distributed Sensor Networks for Electric Utilities Project (Currier, 2009). SDG&E was not involved in this assessment, and the cost effectiveness conclusions presented here do not necessarily represent the views of SDG&E.

This report concluded that the wireless sensor network offers not only new sensing, communications, and wireless mesh network technology but new modes and types of detection and protection, a very low false alarm rate, lower cost of equipment and labor (after the first perimeter and/or level of detection is installed), lower cost of power and communications, and the huge savings of not having to purchase, install, and monitor a CCTV surveillance video system in order to assess if there is a real or potential threat to an asset. The wireless sensor network can be added to, or integrated into, other existing systems like sending their alarm outputs to an existing or future CCTV video surveillance system if video verification is desired, needed or mandated.

The report found that the system is as or more effective and performs as well as or better than alternate technologies, as demonstrated and documented in the active and passive test reports, the SDG&E statement of the daily average false alarm rate of the currently installed systems, and as compared to the specifications and reports of the alternate technologies. It is more expandable, easier to expand, and more cost effective to expand. The system provides a communication infrastructure that allows unique dual-use capabilities beyond security applications, such as monitoring asset state of health. The system allows for monitoring and recording the health not only of its own network but of the sensors and the transmission assets they're monitoring. The radios or motes can be configured, upgraded, or rebooted remotely and additional sensors can be brought "on-line" or added almost instantly.

4.0 Conclusions and Recommendations

This section describes conclusions for this project and makes recommendations for future applications of this technology.

4.1. Conclusions

The system developed by SAIC successfully met the objectives of the project. The system that was demonstrated to the TAC successfully demonstrated that sensor networks based on advanced low-power mesh networks can play an important role in monitoring electric transmission infrastructure to increase the reliability and reduce the cost of power distribution. The system also demonstrated that wireless mesh sensor systems can provide a dual-use capability to monitor the state of health of components of the transmission system.

SDG&E was not involved in the cost effectiveness assessment of the system, and the cost effectiveness conclusions presented here do not necessarily represent the views of SDG&E.

Specifically, this project demonstrated that:

- Wireless mesh networking provides an effective communication framework for operation in power transmission environments, despite the harsh EMI environment due to high voltages and RF obstructions.
- Wireless mesh networking allows very cost-effective installation of a monitoring system.
- Wireless mesh networking allows flexible and cost-effective modification and augmentation of an existing monitoring system.
- Wireless mesh networking provides a cost-effective method for monitoring transmission towers.
- Ultra-low power wireless mesh networking provides low maintenance costs based on multi-year lifetimes using replaceable batteries.
- Fusion of detections from a network of sensors produces very effective detection of intrusions with a very low false alarm rate.

4.2. Recommendations

Working with ENERGY COMMISSION, SDG&E and the TAC, this project was able to demonstrate this system to a relevant and interested user community. We assume an ENERGY COMMISSION goal is to develop technology that eventually gets fielded to improve the security and efficiency of our California utilities. As such, the next step should facilitate production and successful transition to electric utility providers of California.

Utility companies will want to purchase products from vendors, but evolving the current prototype to a production system will require investment. Any private company that considers this investment will need to perform a market analysis and estimate their return on investment (ROI). It is clear that the ROI is improved if the scope of the system can be expanded beyond physical security (e.g., machine health monitoring, environmental monitoring, aircraft warning light state of health, fault current detection, power line temperature, etc.).

The authors recommend a demonstration of a multi-purpose “smart dust” wireless sensor network for the utility industry (including a long linear network, ~10 km, associated with transmission lines) combined with a comprehensive plan for production and transition. The requirements for the demonstration will be provided by utility companies in California, i.e. what would they need to see before they would purchase and deploy sensor networks? The production and transition plan will include a market assessment, ROI, identification of suitable and interested product vendors (in California), producibility, reliability, cost, support planning, IP, teaming agreements, etc. This plan is intended to identify and address all barriers to production and transition.

5.0 References

Abel, A., Government Activities to Protect the Electric Grid, Congressional Research Service Report for Congress, Order Code RS21958, 6 pp., February, 2005.

Anonymous, Internal Reports on Guerrilla Attacks on the National Interconnected System, Interconexion Electrica S.A., Medellin, Colombia, 1988-2004.

Bowman, J.R., D. Wahl and B. Crews, Demonstration System Requirements and Site Survey Report for the Advanced Distributed Sensor Networks for Electric Utilities Project, Science Applications International Corporation, Technical Report SAIC-08/3002, 2008.

Currier, L., Performance and Cost Report for the Advanced Distributed Sensor Networks for Electric Utilities Project, Sidus Solutions Technical Report, 2009.

DHS, Acts of Sabotage Involving High Voltage Transmission Towers, Department of Homeland Security Information Bulletin, http://crypome.org/sabotage-towers.htm , October 30, 2003.

DHS, Science and Technology Directorate, Department of Homeland Security, The National Plan for Research and Development in Support of Critical Infrastructure Protection, http://www.dhs.gov/xlibrary/assets/ST_2004_NCIP_RD_PlanFINALApr05.pdf, p. 25 of 81, 2005.

Hatler, M. and C. Chi, Wireless sensor networks: Growing markets, accelerating demand, ON world emerging wireless research, July 2005.

HSOC, Attempted Sabotage of High Voltage Transmission Lines, Homeland Security Operations Center (HSOC) Incident Report and Request for Information, 30 December 2004.

Office of Energy Assurance, U.S. Department of Energy, Checklist Attachment Version Date: February 22, 2002.

Talbot, D., DARPA's Disruptive Technologies, MIT Technology Review, http://www.technologyreview.com/Biztech/12622, October, 2001.

Wahl, D., Demonstration System Test Plan for the Advanced Distributed Sensor Networks for Electric Utilities Project, Science Applications International Corporation, Technical Report SAIC-08/3009, 2008.

Wahl, D., T. Congdon, J. Hanson and R. Bowman, Demonstration System Test Report for the Advanced Distributed Sensor Networks for Electric Utilities Project, Science Applications International Corporation, Technical Report SAIC-09/3010, 2009.

6.0 Glossary

This section defines acronyms used in the body of the report.

Acronyms	**Definition**
CCTV	Closed Circuit Television
ENERGY COMMISSION	California Energy Commission
DHS	Department of Homeland Security
DOD	Department of Defense
EMI	Electromagnetic Interference
GIS	Gas-insulated Switchgear
GPS	Global Positioning Satellite
GUI	Graphical User Interface
LOS	Line of Sight
PIR	Passive Infrared
RF	Radio Frequency
SAIC	Science Applications International Corporation
SCADA	Supervisory Control And Data Acquisition
SDG&E	San Diego Gas & Electric
TAC	Technical Advisory Committee
TRR	Test Readiness Review